Matematická logika

Ondřej Lengál

Fakulta informačních technologií
Vysoké učení technické v Brně

SDL'21

Logika

(Matematická) logika: oblast matematiky zabývající se univerzálními principy usuzování v různých formálních systémech

- usuzování: základní pravdy, odvozovací pravidla
- formální systém (příklady: algebra, geometrie, program. jazyk)

Logika a informatika

- Logika je základní pilíř informatiky:
  - **hardware**: výroková (Booleova) logika
  - **databáze**: predikátová logika 1. řádu (SQL)
  - **programovací jazyky**: teorie typů (logika vyššího řádu)
  - **softwarové inženýrství**: predikátová logika 1. řádu
  - **verifikace**: předchozí + temporální logiky (LTL/CTL), ...
  - **umělá inteligence**: predikátová logika 1. řádu, modální logiky, ...
  - **syntéza**: predikátová logika 1./2. řádu
  - **kryptografie**: interaktivní/pravděpodobnostní důkazové systémy, zero-knowledge důkazy (kryptoměny)
  - **řízení**: fuzzy logika
  - ...

$$\dfrac{\dfrac{}{\vdash \{y=12\}\ \mathtt{x:=y}\ \{x=12\wedge y=12\}}\,\textsc{Assgn} \qquad \dfrac{\big(x=12\wedge y=12\big)\Rightarrow\big(y=12\wedge(\exists n\in\mathbb{N}: x=2^n(y-2)+2)\wedge(x\le 42)\big) \qquad \dfrac{\dfrac{\dfrac{}{\vdash \{y=12\wedge(\exists n\in\mathbb{N}: x=2^n(y-2)+2)\wedge(x\le 42)\wedge(x<30)\}\ \mathtt{x:=x*2}\ \{y=12\wedge(\exists n\in\mathbb{N}: x=2^n(y-2)+4)\wedge(x\le 44)\}}\,\textsc{Assgn} \quad \dfrac{}{\vdash \{y=12\wedge(\exists n\in\mathbb{N}: x=2^n(y-2)+4)\wedge(x\le 44)\wedge(x<30)\}\ \mathtt{x:=x-2}\ \{y=12\wedge(\exists n\in\mathbb{N}: x=2^n(y-2)+2)\wedge(x\le 42)\}}\,\textsc{Assgn}}{\vdash \{y=12\wedge(\exists n\in\mathbb{N}: x=2^n(y-2)+2)\wedge(x\le 42)\wedge(x<30)\}\ \mathtt{x:=x*2\ ;\ x:=x-2}\ \{y=12\wedge(\exists n\in\mathbb{N}: x=2^n(y-2)+2)\wedge(x\le 42)\}}\,\textsc{Seq}}{\vdash \{y=12\wedge(\exists n\in\mathbb{N}: x=2^n(y-2)+2)\wedge(x\le 42)\}\ \mathtt{while\ (x<30)\ \{x:=x*2\ ;\ x:=x-2\}}\ \{y=12\wedge(\exists n\in\mathbb{N}: x=2^n(y-2)+2)\wedge(x\le 42)\wedge\neg(x<30)\}}\,\textsc{While} \qquad \big(y=12\wedge(\exists n\in\mathbb{N}: x=2^n(y-2)+2)\wedge(x\le 42)\wedge\neg(x<30)\big)\Rightarrow x=42}{\vdash \{x=12\wedge y=12\}\ \mathtt{while\ (x<30)\ \{x:=x*2\ ;\ x:=x-2\}}\ \{x=42\}}\,\textsc{Concl}}{\vdash \{y=12\}\ \mathtt{x\ :=\ y;\ while\ (x<30)\ \{x:=x*2\ ;\ x:=x-2\}}\ \{x=42\}}\,\textsc{Seq}$$

Výroková (Booleova) logika

Výroková logika

Logika je jazyk, má tedy syntaxi a sémantiku.

- **Syntaxe**: určuje, jak se vytvoří fráze jazyka:

$$\begin{aligned}\varphi ::= 0 \mid 1 \mid X \mid (\neg\varphi_1) \mid \\ (\varphi_1 \wedge \varphi_2) \mid (\varphi_1 \vee \varphi_2) \mid \\ (\varphi_1 \rightarrow \varphi_2) \mid (\varphi_1 \leftrightarrow \varphi_2)\end{aligned}$$

  - X je proměnná z množiny proměnných $\mathbb{X}$ (spočetně ∞)

Příklad

- $((X \wedge (\neg Y)) \rightarrow Z)$ **je** formule
- $X(Y \vee Z)$ **není** formule
- $X \wedge Y \vee Z$ **není** formule
- Y **je** formule

(když je priorita jasná, závorky často vynecháváme)

Výroková logika — sémantika

Sémantika určuje co vytvořené fráze znamenají

Ohodnocení proměnných

- funkce $I\colon \mathbb{X} \to \{0, 1\}$
- příklad: $I = \{X \mapsto 1, Y \mapsto 0, \ldots\}$

Sémantika výrokové formule:

- definována induktivně dle pravdivostní tabulky:

φ	ψ	$\neg\varphi$	$\varphi \wedge \psi$	$\varphi \vee \psi$	$\varphi \to \psi$	$\varphi \leftrightarrow \psi$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Výroková logika — sémantika

Příklad

$$\varphi = ((X \wedge (\neg Y)) \to X)$$

X	Y	$\neg Y$	$X \wedge (\neg Y)$	φ
0	0			
0	1			
1	0			
1	1			

- Kolik existuje výrokových formulí nad proměnnými $\{X, Y\}$?
- Kolik existuje výrokových formulí nad proměnnými $\mathbb{X}$?
- Kolik existuje výrokových formulí nad proměnnými $\{X, Y\}$ s různou sémantikou? Tedy, kolik existuje různých logických binárních spojek?

Výroková logika — sémantika

Příklad

$$\psi = ((X \leftrightarrow Y) \rightarrow Z)$$

X	Y	Z	$X \leftrightarrow Y$	ψ
0	0	0		
0	0	1		
0	1	0		
0	1	1		
1	0	0		
1	0	1		
1	1	0		
1	1	1		

- Kolik existuje výrokových formulí nad proměnnými $\{X, Y, Z\}$ s různou sémantikou?

Výroková logika — pojmy

model formule φ:

- je ohodnocení proměnných, které splňuje φ
- značíme $I \models \varphi$
- opak (I nesplňuje φ) značíme $I \not\models \varphi$

splnitelnost (satisfiability):

- formule φ je splnitelná pokud má model
- tj. existuje ohodnocení proměnných I takové, že $I \models \varphi$

Výroková logika — pojmy

platnost (validity):

- formule φ je platná (**tautologie**) pokud $I \models \varphi$ pro všechna ohodnocení I
- značíme $\models \varphi$
- opaku (formule není platná) říkáme neplatnost (značíme $\not\models \varphi$)

kontradikce (nesplnitelnost, unsatisfiability):

- formule φ je kontradikce pokud nemá model
- tj. neexistuje ohodnocení proměnných I takové, že $I \models \varphi$
- **pozor**: $\models \neg\varphi$ není to samé jako $\not\models \varphi$

Platí následující dualita:

- formule φ je platná právě když formule $\neg\varphi$ je nesplnitelná
- formule φ je splnitelná právě když formule $\neg\varphi$ je neplatná

Výroková logika — pojmy

logická ekvivalence:

- formule φ a ψ jsou ekvivalentní pokud je I modelem φ právě když je modelem ψ
- neboli, když je formule $\varphi \leftrightarrow \psi$ tautologie
- značíme $\varphi \Leftrightarrow \psi$

Jaký je rozdíl mezi $\varphi \leftrightarrow \psi$ a $\varphi \Leftrightarrow \psi$?

- $\varphi \leftrightarrow \psi$ je formule výrokové logiky
- $\varphi \Leftrightarrow \psi$ je tvrzení o formulích φ a ψ v metajazyce. **Není** to formule.

logický důsledek:

- formule ψ je logickým důsledkem formule φ pokud každý model φ je i modelem ψ
- neboli, když je formule $\varphi \rightarrow \psi$ tautologie
- značíme $\varphi \Rightarrow \psi$

Podobně jako výše, $\varphi \rightarrow \psi$ a $\varphi \Rightarrow \psi$ **nejsou** to samé.

Výroková logika — Booleova algebra

$(\{0,1\}, \wedge, \vee, \neg, 0, 1)$ tvoří Booleovu algebru.

- rovnost $=$ je definována jako logická ekvivalence $\Leftrightarrow$
- např. $(X \wedge Y) \vee X \; = \; X$

$$
\begin{array}{rcll}
X \wedge (Y \wedge Z) & \Leftrightarrow & (X \wedge Y) \wedge Z & \text{(asociativita)} \\
X \vee (Y \vee Z) & \Leftrightarrow & (X \vee Y) \vee Z & \text{(asociativita)} \\
X \wedge (Y \vee Z) & \Leftrightarrow & (X \wedge Y) \vee (X \wedge Z) & \text{(distributivita)} \\
X \vee (Y \wedge Z) & \Leftrightarrow & (X \vee Y) \wedge (X \vee Z) & \text{(distributivita)} \\
\neg(X \wedge Y) & \Leftrightarrow & \neg X \vee \neg Y & \text{(De Morganovy zákony)} \\
\neg(X \vee Y) & \Leftrightarrow & \neg X \wedge \neg Y & \text{(De Morganovy zákony)}
\end{array}
$$

$$
\begin{array}{rclrcll}
X \vee X & \Leftrightarrow & X & X \wedge X & \Leftrightarrow & X & \text{(idempotence)} \\
X \vee 0 & \Leftrightarrow & X & X \wedge 1 & \Leftrightarrow & X & \text{(neutralita)} \\
X \vee 1 & \Leftrightarrow & 1 & X \wedge 0 & \Leftrightarrow & 0 & \text{(anihilace)} \\
X \wedge \neg X & \Leftrightarrow & 0 & X \vee \neg X & \Leftrightarrow & 1 & \text{(komplementarita)}
\end{array}
$$

Výroková logika — další ekvivalence

$$
\begin{aligned}
X \rightarrow Y \quad &\Leftrightarrow \quad \neg X \vee Y \\
X \rightarrow Y \quad &\Leftrightarrow \quad \neg(X \wedge \neg Y) \\
X \leftrightarrow Y \quad &\Leftrightarrow \quad (X \rightarrow Y) \wedge (Y \rightarrow X)
\end{aligned}
$$

$X \quad \Leftrightarrow \quad \neg\neg X$ (eliminace dvojité negace)

Výroková logika — normální formy

Disjunktivní normální forma (DNF, někdy též *sum of products: SoP*):

- je disjunkce konjunkcí literálů:

$$\bigvee_i \bigwedge_j \ell_{i,j}$$

- literál je proměnná (X) nebo její negace ($\neg X$)

Příklad

Nechť

$$\varphi\colon (P \vee \neg\neg Q) \wedge (R \rightarrow S).$$

Formule

$$\psi\colon (P \wedge \neg R) \vee (P \wedge S) \vee (Q \wedge \neg R) \vee (Q \wedge S)$$

je ekvivalentní formuli φ a je v DNF.

Výroková logika — normální formy

Konjunktivní normální forma (CNF, někdy též *product of sums: PoS*):

- je konjunkce disjunkcí literálů

$$\bigwedge_i \bigvee_j \ell_{i,j}$$

Příklad

Nechť

$$\varphi\colon (P \wedge \neg\neg Q) \vee (R \rightarrow S).$$

Formule

$$\psi\colon (P \vee \neg R \vee S) \wedge (Q \vee \neg R \vee S)$$

je ekvivalentní formuli φ a je v CNF.

Predikátová logika 1. řádu

Predikátová logika

Predikátová logika 1. řádu (First-Order Logic, FOL)

- zabývá se tvrzeními o entitách, jejich vlastnostech a vztazích
- staví na výrokové logice
- interpretuje („dívá se dovnitř“) výroků
- uvažuje entity z univerza—tyto jsou označeny termy zkonstruovanými z proměnných a funkcí, např.
  - x, 5, $f(x, 2)$, $40 + 2$, $\mathit{fatherOf}(\mathit{motherOf}(x))$, $\mathit{head}(\texttt{"abc"})$, $\sin(y)$
- výroky jsou nahrazeny predikáty nad termy, např.
  - $x = y$, $\mathit{even}(x)$, $p(x, y, z)$, $\mathit{isFatherOf}(x, y)$
- zavádí kvantifikátory pro vyjádření vlastností entit z univerza:
  - $\forall x$ — univerzální kvantifikátor (všechny entity x splňují vlastnost)
  - $\exists x$ — existenční kvantifikátor (nějaká entita x splňuje vlastnost)

  (v logice 2. a vyššího řádu se dá kvantifikovat přes relace; zde se tímto zabývat nebudeme)

Predikátová logika

Příklad

- Všichni muži jsou smrtelní. Sokrates je muž. Tedy Socrates je smrtelný.

$$\big(\forall x(man(x) \to mortal(x)) \wedge man(Socrates)\big) \to mortal(Socrates)$$

- Existuje nekonečně mnoho prvočísel.

$$\forall x \exists y\big(y > x \wedge \forall z(z \neq 1 \to \forall w(w \cdot z \neq y))\big)$$

- Relace R je tranzitivní. $\forall x \forall y \forall z(\ (R(x,y) \wedge R(y,z)) \to R(x,z)\ )$
- Uvažujme tabulky `R[jmeno, id]` a `S[id, vek]` v SQL databázi
  `select R.jmeno from R join S on R.id = S.id where S.vek = 42`

$$\exists z(R(x,z) \wedge S(z,42))$$

- Velká Fermatova věta

$$\forall n \forall x \forall y\big(n > 2 \quad \to \quad \forall z(x^n + y^n \neq z^n)\big)$$

Predikátová logika — syntaxe

Syntaxe:

- **Abeceda**:
  - logické spojky: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ (z výrokové logiky)
  - proměnné: $x, y, \ldots, x_1, x_2, \ldots$
  - kvantifikátory: $\forall, \exists$
  - závorky: (,)
  - $\mathcal{F}$: funkční symboly (s $_{/aritou}$): $f_{/2}$, $+_{/2}$, $\sin_{/1}$, $fatherOf_{/1}$, $\pi_{/0}$
    - nulární funkce (arita 0): konstanty
    - použití: $f(a, 3)$, $+(40, 2)$, $\sin(x)$, $fatherOf(Luke)$, $\pi()$
    - často píšeme: $40 + 2$ [pro $+(40, 2)$], π [pro $\pi()$], ...
  - $\mathcal{P}$: predikátové symboly (s $_{/aritou}$): $p_{/3}$, $isJedi_{/1}$, $<_{/2}$
    - použití: $p(a, x, 9)$, $isJedi(Anakin)$, $<(x, \pi)$
    - často píšeme: $x < \pi$ [pro $<(x, \pi)$], ...
  - „vestavěný“ predikátový symbol rovnosti $=_{/2}$
- Signatura $\langle \mathcal{F}, \mathcal{P} \rangle$ = funkční + predikátové symboly
  - může být chápána jako parametr, který se dosadí do šablony
- Jazyk: je jednoznačně dán signaturou

Predikátová logika — syntaxe

Signatura $\langle \mathcal{F}, \mathcal{P} \rangle$ = funkční $+$ predikátové symboly

Příklad

- jazyk teorie uspořádání: $\langle \emptyset, \{<_{/2}\} \rangle$
  - žádný funkční symbol
  - jeden binární predikátový symbol $<$
- jazyk teorie grup: $\langle \{\cdot_{/2}, e_{/0}\}, \emptyset \rangle$
  - binární funkční symbol $\cdot$ (grupová operace násobení)
  - nulární funkční symbol e pro neutrální prvek
- jazyk teorie množin: $\langle \emptyset, \{\in_{/2}\} \rangle$
- jazyk teorie polí: $\langle \{([]_r)_{/2}, ([]_w)_{/3})\}, \emptyset \rangle$
  - binární funkční symbol čtení z pole $[]_r$, např., $A[i]_r$
  - ternární funkční symbol zápisu do pole $[]_w$, např., $A[i, y]_w$ (zápis y na index i v poli A)
- jazyk teorie seznamů: $\langle \{\mathsf{cons}_{/2}, \mathsf{car}_{/1}, \mathsf{cdr}_{/1}\}, \{\mathsf{atom}_{/1}\} \rangle$
- jazyk elementární (tzv. Peanovy) aritmetiky: $\langle \{S_{/1}, 0_{/0}, +_{/2}, \cdot_{/2}\}, \emptyset \rangle$

Predikátová logika — syntaxe

Gramatika:

- term (budou nabývat hodnot z univerza):
  1. Každá proměnná je term.
  2. Pokud je $f_{/n}$ funkční symbol a $t_1, \ldots, t_n$ jsou termy, pak i $f(t_1, \ldots, t_n)$ je term.
  3. Každý term vznikne konečným počtem užití pravidel 1 a 2.
- příklady termů: x, 5, $f(x, 2)$, $40 + 2$, $\mathsf{car}(\mathsf{cons}(x, y))$, $\mathit{head}(\texttt{"abc"})$, $\sin(y)$

Predikátová logika — syntaxe

Gramatika (pokr.):

- atomická formule φ_{atom}:
  - $p(t_1, \ldots, t_n)$ kde $p_{/n}$ je predikátový symbol a $t_1, \ldots, t_n$ jsou termy
  - (platí i pro p „vestavěný" symbol rovnosti $=_{/2}$)
- formule:

$$\begin{aligned}\varphi ::= \varphi_{atom} \mid (\neg\varphi_1) \mid\\ (\varphi_1 \wedge \varphi_2) \mid (\varphi_1 \vee \varphi_2) \mid\\ (\varphi_1 \rightarrow \varphi_2) \mid (\varphi_1 \leftrightarrow \varphi_2) \mid\\ (\forall x \varphi_1) \mid (\exists x \varphi_1)\end{aligned}$$

  - kde x je proměnná z množiny proměnných $\mathbb{X}$
  - (závorky opět často vynecháváme)
- příklady formulí:
  - $\exists x(40 + x = 42 \wedge 40 \cdot x = 80)$,
  - $\forall x(\tan(x) = \frac{\sin(x)}{\cos(x)})$,
  - $\mathsf{atom}(\mathsf{car}(\mathsf{cons}(x, y)))$,
  - $\forall x(\exists y(x = y \cdot y \vee x = -y \cdot y))$

Predikátová logika — syntaxe

výskyty proměnných ve formuli:

- vázaný: výskyt v rozsahu platnosti kvantifikátoru
  - např. $\textsc{Bound}\big[\ \exists x(x = 4 \wedge \neg(y = 5))\ \big] = \{x\}$
- volný: výskyt, který není vázaný žádným kvantifikátorem
  - např. $\textsc{Free}\big[\ x = 4 \wedge (\exists y(y = 5))\ \big] = \{x\}$
- proměnná může mít ve formuli jak vázaný, tak i volný výskyt

Příklad

$$\forall x\big(\ p(f(x), y) \rightarrow \forall y(p(f(x), y))\ \big)$$

- x se vyskytuje jen vázané
- y se vyskytuje volné (antecedent) i vázané (konsekvent)

- často píšeme $\varphi(x_1, \ldots, x_n)$ když $\textsc{Free}\big[\varphi\big] \subseteq \{x_1, \ldots, x_n\}$
  - $x_1, \ldots, x_n$ slouží jako „rozhraní“ k φ
- φ je uzavřená (také *výrok*) když $\textsc{Free}\big[\varphi\big] = \emptyset$

Predikátová logika — sémantika

Sémantika predikátové logiky:

- symboly jazyka dosud **neměly žádný význam**
- složitější než pro výrokovou logiku

Realizace (interpretace): $I = (D_I, \alpha_I)$: dává symbolům význam

- doména (univerzum diskurzu) D_I: neprázná množina
  - např., $\mathbb{N}$, $\{0, 1, 2, 3, 4\}$, $\mathbb{R}^3$, People, $\mathit{List}[\mathbb{N}]$, Σ^*, …
- ohodnocení α_I obsahující:
  - pro každý funkční symbol $f_{/n}$ funkci $f_I : \overbrace{D_I \times \ldots \times D_I}^{n} \to D_I$
    - např., $\alpha_I(+) = \{(0,0) \mapsto 0, (0,1) \mapsto 1, (1,0) \mapsto 1, (1,1) \mapsto 2, \ldots\}$
    - pro konstanty tedy 1 hodnotu, např., $\alpha_I(\pi) = \{() \mapsto 3.14\}$
  - pro každý predikátový symbol $p_{/n}$ relaci $p_I \subseteq \overbrace{D_I \times \ldots \times D_I}^{n}$
    - např., $\alpha_I(<) = \{(0,1), (0,2), (1,2), \ldots\}$
    - např., $\alpha_I(\mathit{even}) = \{0, 2, 4, \ldots\}$
    - např., $\alpha_I(\mathit{edge}) = \{(v_1, v_2), (v_2, v_3), \ldots\}$
  - ohodnocení proměnných z $\mathbb{X}$ na hodnotu z D_I, např., $x \mapsto 42$

Predikátová logika — realizace

Příklad

Příklady realizací jazyka se signaturou $\langle \mathcal{F} = \{+_{/2}\}, \mathcal{P} = \emptyset \rangle$:

- Sčítání v $\mathbb{N}$: $I = (\mathbb{N}, \alpha_I)$ kde
  - $\alpha_I(+) = (+_{\mathbb{N}})$ (sčítání přirozených čísel)
- Sčítání v $\mathbb{R}^3$: $I = (\mathbb{R}^3, \alpha_I)$ kde
  - $\alpha_I(+) = \{((x_1, y_1, z_1), (x_2, y_2, z_2)) \mapsto (x_1 +_{\mathbb{R}} x_2, y_1 +_{\mathbb{R}} y_2, z_1 +_{\mathbb{R}} z_2) \mid \ldots\}$
- Modulární sčítání v $\{0, 1, 2\}$: $I = (\{0, 1, 2\}, \alpha_I)$ kde
  - $\alpha_I(+) = \{(x, y) \mapsto (x + y \mod 3) \mid x, y \in \{0, 1, 2\}\}$

Predikátová logika— realizace

Příklad

Příklady realizací jazyka se signaturou $\langle \mathcal{F} = \{+_{/2}, \cdot_{/2}, {}^*{}_{/1}\}, \mathcal{P} = \{E_{/1}\}\rangle$:

- Sjednocení, konkatenace a iterace množin řetězců nad Σ: $I = (2^{\Sigma^*}, \alpha_I)$ kde
  - $\alpha_I(+) = \{(x, y) \mapsto (x \cup y) \mid x, y \subseteq \Sigma^*\}$
  - $\alpha_I(\cdot) = \big\{(x, y) \mapsto \{uv \mid u \in x, v \in y\} \mid x, y \subseteq \Sigma^*\big\}$
  - $\alpha_I(^*) = \big\{x \mapsto \bigcup_{i \geq 0} \{u^i \mid u \in x\} \mid x \subseteq \Sigma^*\big\}$
  - $\alpha_I(E) = \big\{\{\epsilon\}\big\}$
- Disjunkce, konjunkce a negace v Booleově algebře: $I = (\{0, 1\}, \alpha_I)$ kde
  - $\alpha_I(+) = \{(0, 0) \mapsto 0, (0, 1) \mapsto 1, (1, 0) \mapsto 1, (1, 1) \mapsto 1\}$
  - $\alpha_I(\cdot) = \{(0, 0) \mapsto 0, (0, 1) \mapsto 0, (1, 0) \mapsto 0, (1, 1) \mapsto 1\}$
  - $\alpha_I(^*) = \{0 \mapsto 1, 1 \mapsto 0\}$
  - $\alpha_I(E) = \{0\}$

Predikátová logika — sémantika

hodnota termu t **v realizaci** I: definována induktivně následujícím rozšířením $\alpha_I[t]$:

$$\alpha_I[f(t_1, \ldots, t_n)] \stackrel{\text{def}}{=} \alpha_I[f](\alpha_I[t_1], \ldots, \alpha_I[t_n])$$

pro $f_{/n}$ ($\alpha_I[x]$ pro $x \in \mathbb{X}$ a $\alpha_I[c]$ pro konstantu $c_{/0}$ jsou již definovány v realizaci I)

Predikátová logika — sémantika

Příklad

Uvažujme jazyk se signaturou $\langle \mathcal{F} = \{+_{/2}, S_{/1}, Z_{/0}\}, \mathcal{P} = \emptyset \rangle$ a následující term:

$$t: \qquad x + S(x + Z)$$

Určete hodnotu termu t v následujících realizacích:

- Sčítání v $\mathbb{N}$: $I = (\mathbb{N}, \alpha_I)$ kde

  $\alpha_I(+) = (+_\mathbb{N})$ (sčítání přirozených čísel)

  $\alpha_I(S) = \{x \mapsto x +_\mathbb{N} 1_\mathbb{N}\}_{x \in \mathbb{N}}$ (funkce následníka)

  $\alpha_I(Z) = 0_\mathbb{N}$ (nula)

  $\alpha_I(x) = 42_\mathbb{N}$

Predikátová logika — sémantika

Příklad

Uvažujme jazyk se signaturou $\langle \mathcal{F} = \{+_{/2}, S_{/1}, Z_{/0}\}, \mathcal{P} = \emptyset\rangle$ a následující term:

$$t: \qquad x + S(x + Z)$$

Určete hodnotu termu t v následujících realizacích:

- Množinové operace v $2^{\mathbb{N}}$: $I = (2^{\mathbb{N}}, \alpha_I)$ kde
  $\alpha_I(+) = (\cup)$ (sjednocení množin)
  $\alpha_I(S) = \{x \mapsto x \cup \{1_{\mathbb{N}}\}\}_{x \in 2^{\mathbb{N}}}$ (přídání prvku $1_{\mathbb{N}}$ do množiny)
  $\alpha_I(Z) = \emptyset$ (prázdná množina)
  $\alpha_I(x) = \{1_{\mathbb{N}}, 42_{\mathbb{N}}\}$

Predikátová logika — sémantika

sémantika formule φ predikátové logiky:

- určuje, zda v dané realizaci I formule platí ($I \models \varphi$), nebo ne ($I \not\models \varphi$)
- definována induktivně:
  1. pro predikátový symbol $p_{/n}$ a termy $t_1, \dots, t_n$ platí

     $$I \models p(t_1, \dots, t_n) \qquad \text{právě když} \qquad \alpha_I[p](\alpha_I[t_1], \dots, \alpha_I[t_n])$$

     (pro rovnost: $I \models t_1 = t_2$ právě když $\alpha_I[t_1]$ a $\alpha_I[t_2]$ značí stejný prvek z D_I)
  2. pro výrokové spojky:

     $I \models \neg\psi$ právě když $I \not\models \psi$
     $I \models \psi_1 \wedge \psi_2$ právě když $I \models \psi_1$ a zároveň $I \models \psi_2$
     $I \models \psi_1 \vee \psi_2$ právě když $I \models \psi_1$ nebo $I \models \psi_2$
     $I \models \psi_1 \rightarrow \psi_2$ právě když pokud $I \models \psi_1$ pak $I \models \psi_2$
     $I \models \psi_1 \leftrightarrow \psi_2$ právě když $I \models \psi_1$ a zároveň $I \models \psi_2$, nebo $I \not\models \psi_1$ a zároveň $I \not\models \psi_2$
  3. pro kvantifikátory:
     - variant $I \triangleleft \{x \mapsto v\}$ realizace I je realizace získaná z I nahrazením $x \mapsto ?$ za $x \mapsto v$ v α_I
     - $I \models \forall x\varphi$ právě když pro všechny prvky $v \in D_I$ platí $I \triangleleft \{x \mapsto v\} \models \varphi$
       $I \models \exists x\varphi$ právě když existuje prvek $v \in D_I$ takový, že $I \triangleleft \{x \mapsto v\} \models \varphi$

Predikátová logika — pojmy

model formule φ:

- je realizace I taková, že $I \models \varphi$

splnitelnost (satisfiability):

- formule φ je splnitelná pokud má model
- tj. existuje realizace I s doménou D_I a ohodnocením funkčních, predikátových symbolů a proměnných α_I takové, že $I \models \varphi$

Predikátová logika — pojmy

logická platnost:

- formule φ je logicky platná pokud platí pro **všechny** realizace daného jazyka, tj. pro všechny domény a ohodnocení funkčních, predikátových symbolů a proměnných
- značíme $\models \varphi$
- (výroková logika: *tautologie*)

Predikátová logika — pojmy

logická platnost:

- formule φ je logicky platná pokud platí pro **všechny** realizace daného jazyka, tj. pro všechny domény a ohodnocení funkčních, predikátových symbolů a proměnných
- značíme $\models \varphi$
- (výroková logika: *tautologie*)

Příklad

Je následující formule platná?

$$\varphi\colon 1 + 1 = 2$$

proč?

- existují realizace, kde φ neplatí
  - např., $I = \langle \mathbb{N}, \alpha_I \rangle$ kde $\alpha_I(+) = \{\dots, (1,1) \mapsto 3, \dots\}$
- většinou chceme omezit množinu uvažovaných realizací $\varphi \rightsquigarrow$ **teorie** (jazyk + axiomy)

Predikátová logika — pojmy

logická ekvivalence:

- formule φ a ψ jsou logicky ekvivalentní jestliže pro libovolnou realizaci I daného jazyka platí $I \models \varphi$ právě když $I \models \psi$
- neboli, když je formule $\varphi \leftrightarrow \psi$ logicky platná
- značíme $\varphi \Leftrightarrow \psi$

logický důsledek:

- formule ψ je logickým důsledkem formule φ jestliže pokud pro realizaci I platí $I \models \varphi$, pak platí i $I \models \psi$
- neboli, když je formule $\varphi \rightarrow \psi$ logicky platná
- značíme $\varphi \Rightarrow \psi$

Predikátová logika — ekvivalence

$$
\begin{array}{rcll}
\forall x(\neg\varphi) & \Leftrightarrow & \neg\exists x\varphi & \\
\exists x(\neg\varphi) & \Leftrightarrow & \neg\forall x\varphi & \\
(\forall x(\varphi(x))) \wedge (\forall y(\psi(y))) & \Leftrightarrow & \forall x(\varphi(x) \wedge \psi(x)) & \text{pokud } x \notin \textsc{Free}[\psi] \\
(\exists x(\varphi(x))) \vee (\exists y(\psi(y))) & \Leftrightarrow & \exists x(\varphi(x) \vee \psi(x)) & \text{pokud } x \notin \textsc{Free}[\psi] \\
\forall x\varphi & \Leftrightarrow & \varphi & \text{pokud } x \notin \textsc{Free}[\varphi] \\
\exists x\varphi & \Leftrightarrow & \varphi & \text{pokud } x \notin \textsc{Free}[\varphi] \\
\forall x(\varphi \vee \psi) & \Leftrightarrow & (\forall x\varphi) \vee \psi & \text{pokud } x \notin \textsc{Free}[\psi] \\
\exists x(\varphi \wedge \psi) & \Leftrightarrow & (\exists x\varphi) \wedge \psi & \text{pokud } x \notin \textsc{Free}[\psi]
\end{array}
$$